The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:

11/11/2014

SUBJECT:

Vulnerability in Microsoft Office Could Allow Remote Code Execution (MS14-069)

EXECUTIVE SUMMARY:

A vulnerability has been discovered in Microsoft Office that could allow a remote attacker to take complete control of a vulnerable system. This vulnerability can be exploited if a user opens a specially crafted file in Microsoft Office 2007.

Successful exploitation could allow an attacker to gain the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

THREAT INTELLIGENCE

There are currently no reports of this vulnerability being exploited in the wild.

SYSTEMS AFFECTED:

- Microsoft Office 2007 Service Pack 3
- Microsoft Word Viewer
- Microsoft Office Compatibility Pack Service Pack 3

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

TECHNICAL SUMMARY:

A vulnerability has been discovered in Microsoft Office that could allow a remote attacker to take complete control of a vulnerable system. The vulnerability exists because Microsoft Word does not properly handle objects in memory while parsing specially crafted Office files. An attacker could create a specially crafted file and entice a user to open it in order to exploit this vulnerability.

Successful exploitation could allow an attacker to gain the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Remind users not to download, accept, or execute media files from un-trusted or unknown sources.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

REFERENCES:

Microsoft:

http://technet.microsoft.com/library/security/MS14-069

CVE:

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6333

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6334

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6335